AMENDMENTS TO THE CLAIMS

Claims 1-3 (Cancelled)

4.   (Currently Amended) A method comprising:

identifying a first and a second radio protocol;

receiving the first and second radio protocols protocol;

prior to downloading the first and second radio protocols to a baseband

   module protocol by a vendor, determining whether the first and second

   radio protocols meet protocol meets certification requirements of a third-

   party certification authority prior to the radio protocol being distributed to

   the vendor;

providing guarantees regarding the certification requirements to a relevant

   authority; and

if the first and second radio protocols meet the certification requirements,

   downloading the first and second radio protocols to protocol at a non-

   volatile memory device at a coupled to the baseband module, wherein the

   baseband module is to operate under both the first and second radio

   protocols if the radio protocol meets the certification requirements.

5.   (Currently Amended) The method of claim 4, wherein the determining of the

radio protocol first and second radio protocols meeting the certification

requirements comprises authenticating the radio protocol first and second radio

protocols using a first cryptographic key stored at the baseband module.

6.   (Previously Presented) The method of claim 5, wherein the first cryptographic key

comprises a public key.

7. (Currently Amended) The method of claim 1, wherein the downloading of the ~~radio protocol~~first and second radio protocols comprises writing the ~~radio protocol~~first and second radio protocols to the non-volatile memory device via a boot loader program.

8. (Previously Presented) The method of claim 7, further comprising determining whether the boot loader program is approved by a manufacturer of the baseband module.

9. (Previously Presented) The method of claim 8, wherein the determining whether the boot loader program is approved by the manufacturer comprises authenticating the program using a second cryptographic key stored at the baseband module.

10. (Previously Presented) The method of claim 9, wherein the second cryptographic key comprises a public key.

Claims 11-15 (Cancelled)

16. (Currently Amended) A system comprising:

a receiver to receive and identify a <u>first and a second</u> radio protocol;

a mechanism to:

prior to downloading the <u>first and second</u> radio <u>protocols to a baseband module</u>~~protocol by a vendor~~, determine whether the <u>first and second</u> radio <u>protocols meet</u>~~protocol meets~~ certification requirements of a third-party certification authority ~~prior to the radio protocol being distributed to the vendor~~, and

provide guarantees regarding the certification requirements to a relevant authority; and

a non-volatile memory device ~~at a~~ coupled to the baseband module to accept a

download of and store the first and second radio protocols ~~protocol and~~

~~store the radio protocol~~, if the first and second radio protocols meet the

certification requirements, wherein the baseband module is to operate

under both the first and second radio protocols ~~protoco~~.

17. (Currently Amended) The system of claim 16, wherein the mechanism is further

to authenticate the ~~radio protocol~~first and second radio protocols using a first

cryptographic key stored at the baseband module.

18. (Previously Presented) The system of claim 17, wherein the first cryptographic

key comprises a public key.

19. (Currently Amended) The system of claim 16, wherein the ~~radio protocol is~~first

and second radio protocols are downloaded at the non-volatile memory device via

a boot loader program.

20. (Previously Presented) The system of claim 19, wherein the mechanism is further

to determine whether the boot loader program is approved by a manufacturer of

the baseband module.

21. (Previously Presented) The system of claim 20, wherein the mechanism is further

authenticate the boot loader program using a second cryptographic key stored at

the baseband module.

22. (Previously Presented) The system of claim 21, wherein the second cryptographic

key comprises a public key.

23. (Currently Amended) A machine-readable medium ~~having stored thereon sets of~~

comprising instructions which~~,~~ when executed ~~by a machine~~, cause ~~the~~ a machine

to:

identify a first and a second radio protocol;

receive the first and second radio protocols ~~protocol~~;

prior to downloading the first and second radio protocols to a baseband

module~~protocol by a vendor~~, determine whether the first and second radio

protocols meet ~~protocol meets~~ certification requirements of a third-party

certification authority ~~prior to the radio protocol being distributed to the~~

~~vendor~~;

provide guarantees regarding the certification requirements to a relevant

authority; and

if the first and second radio protocols meet the certification requirements,

download the first and second radio protocols to ~~protocol at~~ a non-volatile

memory device ~~at a~~ coupled to the baseband module, wherein the

baseband module is to operate under both the first and second radio

protocols ~~if the radio protocol meets the certification requirements~~.

24.   (Currently Amended) The machine-readable medium of claim 23, wherein the

instructions when executed to ~~determining of~~ determine the ~~radio protocol~~first and

second radio protocols meeting the certification requirements ~~comprises~~ causes

the machine to ~~authenticating~~ authenticate the ~~radio protocol~~first and second radio

protocols using a first cryptographic key stored at the baseband module.

25.   (Previously Presented) The machine-readable medium of claim 24, wherein the

first cryptographic key comprises a public key.

26.   (Currently Amended) The machine-readable medium of claim 23, wherein the

downloading of the first and second radio protocols comprises writing the ~~radio~~

~~protocol~~first and second radio protocols to the non-volatile memory device via a boot loader program.

27.   (Currently Amended) The machine-readable medium of claim 26, wherein the ~~sets of~~ instructions when further executed, ~~further~~ cause the machine to determine whether the boot loader program is approved by the manufacturer of the baseband module.

28.   (Currently Amended) The machine-readable medium of claim 27, wherein the ~~sets of~~ instructions when further executed, ~~further~~ cause the machine to authenticate the boot loader program via a second cryptographic key stored at the baseband module.

29.   (Previously Presented) The machine-readable medium of claim 28, wherein the second cryptographic key comprises a public key.

Claims 30-36 (Cancelled)